(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 580 953 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.09.2005 Bulletin 2005/39

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/58

(21) Application number: **04006851.2**

(22) Date of filing: **22.03.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventors:
- **Brown, Michael K.**
  Peterborough, Ontario K9K 2E4 (CA)
- **Brown, Michael S.**
  Waterloo, Ontario N2K 4B1 (CA)
- **Adams, Neil P.**
  Waterloo, Ontario N2K 4E4 (CA)

(74) Representative: **Jones Day**
Rechtsanwälte, Attorneys-at-Law,
Patentanwälte
Prinzregentenstrasse 11
80538 München (DE)

(54) System and method for viewing message attachments

(57) Methods and systems for handling attachments on wireless mobile communication devices. An attachment provided with a secure message is received at a message server. The secure message itself was received by the server as an attachment. The secure message is processed in order to locate within the secure message the requested attachment. The located attachment is provided to a mobile device.

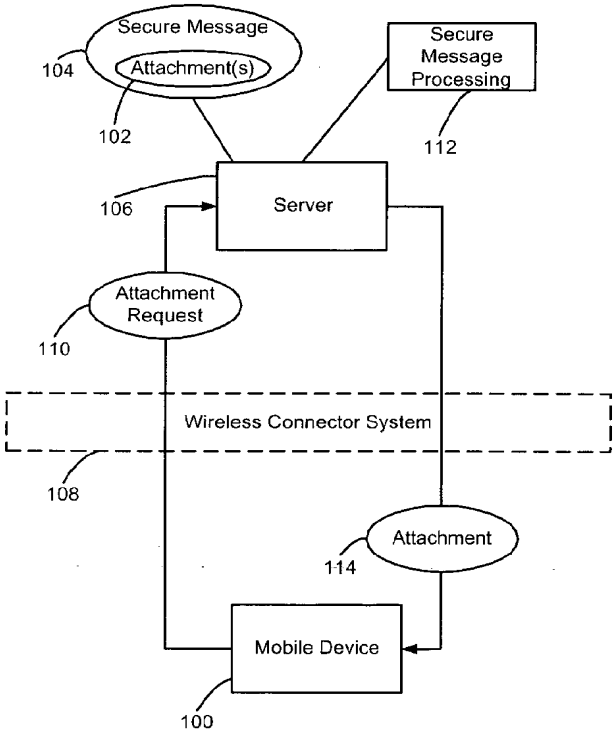

FIG. 3

EP 1 580 953 A1

Description

BACKGROUND

Technical Field

[0001] The present invention relates generally to the field of secure electronic messaging, and in particular to accessing message attachments.

Description of the Related Art

[0002] Capabilities of wireless mobile communication devices have expanded greatly. For example, such devices not only receive electronic messages, but can view attachments associated with electronic messages. However, difficulties arise when a mobile device wishes to access attachments of secure messages. This is due at least in part to how messages and attachments are structured in order to comport with a security scheme.

SUMMARY

[0003] In accordance with the teachings disclosed herein, methods and systems are provided for handling attachments on wireless mobile communication devices. As an example, a method can include receiving an attachment provided with a secure message, wherein the secure message itself was received by the server as an attachment. The secure message is processed in order to locate within the secure message the requested attachment. The located attachment is provided to the mobile device.

[0004] As another example, a system can include a server having a data store that stores a secure message and its associated attachment. The secure message contains a secure layer such that the secure message is received by the server as an attachment itself. A secure message processing module looks into the secure message through the secure layer in order to locate the attachment. The located attachment is provided to the mobile device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005]

Fig. 1 is a block diagram of a messaging system.
Fig. 2 is a block diagram illustrating a secure e-mail message exchange in a messaging system.
Fig. 3 is a block diagram illustrating a mobile device accessing an attachment.
Fig. 4 is a flow chart depicting an operational scenario wherein a mobile device accesses an attachment.
Fig. 5 is a block diagram illustrating a mobile device receiving a rendered attachment.
Fig. 6 is a block diagram illustrating a mobile device providing a key to a server for use in accessing an attachment.
Fig. 7 is a block diagram of a wireless mobile communication device.

DETAILED DESCRIPTION

[0006] The attachment accessing methods and systems disclosed herein may be used with many different types of secure messaging schemes. As an illustration, in a public key cryptography scheme, each user has a key pair including a public key that is distributed or available to other users and a private key that is known only to the user that is the "owner" of the key pair. For secure messaging operations based on public key cryptography, a user uses a private key to decrypt received encrypted messages and to sign messages to be sent. Public keys are used to encrypt messages to be sent and to verify digital signatures on received messages. Thus, access to public keys of other users is required for different secure messaging operations.

[0007] Secure messages may be signed with a digital signature, encrypted, or both signed and encrypted, and may also be processed in other ways by a message sender or intermediate system between a message sender and a messaging client which receives the secure message. For example, secure messages include messages that have been signed, encrypted and then signed, or signed and then encrypted, by a message sender according to variants of Secure Multipurpose Internet Mail Extensions (S/MIME). A secure message could similarly be encoded, compressed or otherwise processed either before or after being signed and/or encrypted.

[0008] A messaging client allows a system on which it operates to receive and possibly also send messages. Messaging clients operate on a computer system, a handheld device, or any other system or device with communications capabilities. Many messaging clients also have additional non-messaging functions.

[0009] Fig. 1 is a block diagram of a messaging system. The system 10 includes a Wide Area Network (WAN) 12, coupled to a computer system 14, a wireless network gateway 16, and a Local Area Network (LAN) 18 (e.g., a corporate LAN). The wireless network gateway 16 is also coupled to a wireless communication network 20, in which a wireless mobile communication device 22 ("mobile device") is configured to operate.

[0010] The computer system 14 is a desktop or laptop personal computer (PC), which is configured to communicate to the WAN 12, which is the Internet in most implementations. PCs, such as computer system 14, normally access the Internet through an Internet Service Provider (ISP), an Application Service Provider (ASP), or the like.

[0011] The LAN 18 is a network-based messaging client. It is normally located behind a security firewall 24. Within the LAN 18, a message server 26, operating on

a computer behind the firewall 24, serves as the primary interface for the corporation to exchange messages both within the LAN 18, and with other external messaging clients via the WAN 12. Two known message servers 26 are Microsoft™ Exchange server and Lotus Domino™ server. These servers 26 are often used in conjunction with Internet mail routers that route and deliver mail messages. A server such as the message server 26 also typically provides additional functionality, such as dynamic database storage for calendars, todo lists, task lists, e-mail, electronic documentation, etc.

[0012] The message server 26 provides messaging capabilities to the corporation's networked computer systems 28 coupled to the LAN 18. A typical LAN 18 includes multiple computer systems 28, each of which implements a messaging client, such as Microsoft Outlook™, Lotus Notes, etc. Within the LAN 18, messages are received by the message server 26, distributed to the appropriate mailboxes for user accounts addressed in the received message, and then accessed by a user through a computer system 28 operating as a messaging client.

[0013] The wireless gateway 16 provides an interface to a wireless network 20, through which messages are exchanged with a mobile device 22. Such functions as addressing of the mobile device 22, encoding or otherwise transforming messages for wireless transmission, and any other required interface functions are performed by the wireless gateway 16. Although the wireless gateway 16 operates with the single wireless network 20 in Fig. 1, wireless gateways may be configured to operate with more than one wireless network in alternative embodiments, in which case the wireless gateway may also determine a most likely network for locating a given mobile device user and may also track users as they roam between countries or networks.

[0014] Any computer system 14, 28 with access to the WAN 12 may exchange messages with a mobile device 22 through the wireless network gateway 16. Alternatively, private wireless network gateways, such as wireless Virtual Private Network (VPN) routers, could be implemented to provide a private interface to a wireless network. For example, a wireless VPN router implemented in the LAN 18 would provide a private interface from the LAN 18 to one or more mobile devices such as the mobile device 22 through the wireless network 20. Wireless VPN routers and other types of private interfaces to the mobile device 22 may effectively be extended to entities outside the LAN 18 by providing a message forwarding or redirection system that operates with the message server 26. Such a redirection system is disclosed in United States Patent No. 6,219,694, which is hereby incorporated into this application by reference. In this type of redirection system, incoming messages received by the message server 26 and addressed to a user of a mobile device 22 are sent through the wireless network interface, either a wireless VPN router, wireless gateway 16 or other interface, to the wireless network 20 and to the user's mobile device 22. Another alternate interface to a user's mailbox on a message server 26 is a Wireless Application Protocol (WAP) gateway, through which a list of messages in a user's mailbox on the message server 26, and possibly each message or a portion of each message, could be sent to the mobile device 22.

[0015] Wireless networks such as the wireless network 20 normally deliver information to and from mobile devices via RF transmissions between base stations and the mobile devices. The wireless network 20 may, for example, be a data-centric wireless network, a voice-centric wireless network, or a dual-mode network that can support both voice and data communications over the same infrastructure. Known data-centric network include the Mobitex™ Radio Network ("Mobitex"), and the DataTAC™ Radio Network ("DataTAC"). Examples of known voice-centric data networks include Personal Communication Systems (PCS) networks like Global System for Mobile Communications (GSM) and Time Division Multiple Access (TDMA) systems. Dual-mode wireless networks include Code Division Multiple Access (CDMA) networks, General Packet Radio Service (GPRS) networks, and so-called third-generation (3G) networks, such as Enhanced Data rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS), which are currently under development.

[0016] The mobile device 22 is a data communication device, a voice communication device, or a multiple-mode device capable of voice, data and other types of communications. An exemplary mobile device 22 is described in further detail below.

[0017] Perhaps the most common type of messaging currently in use is e-mail. In a standard e-mail system, an e-mail message is sent by an e-mail sender, possibly through a message server and/or a service provider system, and is then routed through the Internet, when necessary, to one or more message receivers. E-mail messages are normally sent in the clear and typically use Simple Mail Transfer Protocol (SMTP) headers and Multi-purpose Internet Mail Extensions (MIME) body parts to define the format of the e-mail message.

[0018] In recent years, secure messaging techniques have evolved to protect both the content and integrity of messages, such as e-mail messages. S/MIME and Pretty Good Privacy™ (PGP™) are two public key secure e-mail messaging protocols that provide for both encryption, to protect data content, and signing, which protects the integrity of a message and provides for sender authentication by a message receiver. In addition to utilizing digital signatures and possibly encryption, secure messages may also be encoded, compressed or otherwise processed.

[0019] Fig. 2 is a block diagram illustrating a secure e-mail message exchange in a messaging system. The system includes an e-mail sender 30 coupled to a WAN 32, and a wireless gateway 34, which provides an inter-

face between the WAN 32 and a wireless network 36. A mobile device 38 is adapted to operate within the wireless network 36.

[0020] The e-mail sender 30 is a PC, such as the system 14 in Fig. 1, a network-connected computer, such as computer 28 in Fig. 1, or a mobile device, on which a messaging client operates to enable e-mail messages to be composed and sent. The WAN 32, wireless gateway 34, wireless network 36 and mobile device 38 are substantially the same as similarly-labelled components in Fig. 1.

[0021] In an example digital signature scheme, a secure e-mail message sender 30 digitally signs a message by taking a digest of the message and signing the digest using the sender's private key. A digest may, for example, be generated by performing a check-sum, a Cyclic Redundancy Check (CRC), a hash, or some other non-reversible operation on the message. This digest is then digitally signed by the sender using the sender's private key. The private key is used to perform an encryption or some other transformation operation on the digest to generate a digest signature. A digital signature, including the digest and the digest signature, is then appended to the outgoing message. In addition, a digital Certificate (Cert) of the sender, which includes the sender's public key and sender identity information that is bound to the public key with one or more digital signatures, and possibly any chained Certs and Certificate Revocation Lists (CRLs) associated with the Cert and any chained Certs, is often included with the outgoing message.

[0022] The secure e-mail message 40 sent by the e-mail sender 30 includes a component 42 including the sender's Cert, Cert chain, CRLs and digital signature and the signed message body 44. In the S/MIME secure messaging technique, Certs, CRLs and digital signatures are normally placed at the beginning of a message as shown in Fig. 2, and the message body is included in a file attachment. Messages generated by other secure messaging schemes may place message components in a different order than shown or include additional and/or different components. For example, a signed message 40 may include addressing information, such as "To:" and "From:" email addresses, and other header information not shown in Fig. 2.

[0023] When the secure e-mail message 40 is sent from the e-mail sender 30, it is routed through the WAN 32 to the wireless gateway 34, through the wireless network 36, and then to the mobile device 38. As described above, an e-mail message sender may alternatively send a message directly to a wireless gateway, to a computer system associated with a mobile device, or to a wireless VPN router or other interface for delivery to a mobile device.

[0024] The receiver of the signed message 40, the mobile device 38, typically verifies the digital signature 42 in the secure message 40 by generating a digest of the message body 44, extracting the transmitted digest from the digital signature 42, comparing the generated digest with the digest extracted from the digital signature 42, and then verifying the digest signature in the digital signature. The digest algorithm used by a secure message receiver to generate the generated digest is the same as the algorithm used by the message sender, and is normally specified in a message header, or possibly in a digital signature of the secure message. Commonly used digest algorithm include the Secure Hash Algorithm 1 (SHA1) and Message-Digest Algorithm 5 (MD5), although other digest algorithms may be used. It should be appreciated that the systems and methods described herein are in no way limited to the above, or any other digital signature scheme.

[0025] In order to verify the digest signature, the receiver 38 retrieves the public key of the sender 30, generally by extracting the public key from the sender's Cert 42 attached to the message 40, and then verifies the signature on the digest in the digital signature by performing a reverse transformation on the digest signature. For example, if the message sender 30 generated the digest signature by encrypting the digest using its private key, then a receiver 38 uses the sender's public key to decrypt the digest signature to recover the original digest. The secure message 40 shown in Fig. 2 includes the sender's Cert 42, from which the sender's public key can be extracted. Where the sender's public key was extracted from an earlier message from the sender 30 and stored in a key store in the receiver's local store, the sender's public key may instead be retrieved from the local store. Alternatively, the public key may be retrieved from the sender's Cert stored in a local store, or from a Public Key Server (PKS). A PKS is a server that is normally associated with a Certificate Authority (CA) from which a Cert for an entity, including the entity's public key, is available. A PKS might reside within a corporate LAN such as 18 (Fig. 1), or anywhere on the WAN 32, Internet or other network or system through which message receivers may establish communications with the PKS.

[0026] The Cert, Cert chain and CRLs 42 are used by a receiver to ensure that the sender's Cert is valid, i.e., that the Cert has not been revoked or expired, and is trusted. A Cert is often part of a Cert chain, which includes a user's Cert as well as other Certs to verify that the user's Cert is authentic. For example, a Cert for any particular entity typically includes the entity's public key and identification information that is bound to the public key with a digital signature. Several types of Cert currently in use include, for example, X.509 Certs, which are typically used in S/MIME, and PGP Certs, which have a slightly different format. The digital signature in a Cert is generated by the issuer of the Cert, and is checked by a message receiver as described above. A Cert may include an expiry time or validity period from which a messaging client determines if the Cert has expired. When a CRL is available, the Cert is checked against the CRL to ensure that the Cert has not been

revoked.

[0027] If the digital signature in a message sender's Cert is verified, the Cert has not expired or been revoked, and the issuer of the Cert is trusted by a message receiver, then the digital signature of the message is trusted by the message receiver. If the issuer of the Cert is not trusted, then the message receiver traces a certification path through the Cert chain to verify that each Cert in the chain was signed by its issuer, whose Cert is next in the Cert chain, until a Cert is found that was signed by a root Cert from a trusted source, such as a large PKS. Once a root Cert is found, then a signature can be trusted, because both the sender and receiver trust the source of the root Cert.

[0028] If a secure message was encrypted or otherwise processed by a message sender after being signed, then each receiver first decrypts or performs other inverse processing operations on the message before signature verification is performed. Where encryption or other processing was performed before signing, however, inverse processing such as decryption is performed after signature verification. Encryption and decryption involve applying a cryptographic key and cipher algorithm to information to be encrypted or decrypted. Encryption and decryption use corresponding cipher algorithms, which may or may not be the same, and either the same or different cryptographic keys. In public key systems, different keys are used for encryption and decryption, whereas in "shared secret" type operations, the same key, a secret shared between a sender and recipient, is used for both encryption and decryption.

[0029] Access to a user's public key is also used when an outgoing message addressed to that user is to be encrypted according to a public key encryption algorithm. However, when an error is encountered during a public key access operation, known messaging clients provide little or no information as to the nature of any errors and possible solutions.

[0030] Fig. 3 illustrates a mobile device 100 wishing to access an attachment 102 that is attached to a secure message 104. In Fig. 3, the secure message scheme used in this example treats the secure message 104 itself as an attachment. As an illustration, when a server 106 receives an S/MIME message 104, the S/MIME message 104 is (at least initially) perceived by the server 106 as an attachment due to how the S/MIME message 104 is structured. Such a scheme may be considered as having an attachment 102 within another attachment (i.e., the secure message 104).

[0031] A reason that a secure message 104 appears as an attachment to an e-mail program (e.g., Microsoft Outlook) or to the server 106 is that the message has been enveloped (e.g., encrypted or otherwise protected) with a secure layer. For example, the secure layer can result from the message being encrypted using a random symmetric key, wherein that symmetric key may then be encrypted using the recipient's public key and sent along with the message. If a message is being sent to multiple recipients, the symmetric key is encrypted separately by every recipient's public key. The enveloped message and the encrypted symmetric keys are packaged together and also may be protected via a digital signature.

[0032] More specifically, since S/MIME is used to secure MIME entities, a MIME entity that is secured as such can be thought of as the "inside" MIME entity. That is, it is the "innermost" object of a larger MIME message. One or more attachments may be contained within a MIME entity. These aspects are further discussed in RFC 2633 (version 3) entitled "S/MIME Version 3 Message Specification." It should be understood that message security techniques other than S/MIME may be used that result in a secure layer that envelops or wraps message components and which need to be processed by the systems and methods disclosed herein.

[0033] An attachment 102 contained within a secure message 104 that a mobile device 100 wishes to obtain may be any type of file, such as a textual/word processing document. The attachment 102 may also be an image, audio or video file.

[0034] Because the mobile device 100 is typically resource-limited and in order to save bandwidth, the message server 106 may elect not to initially send the attachment 102 to the mobile device 100 over a wireless connector system 108. While viewing the message on the mobile device 100, a user can request that the message's associated attachment data 102 be transmitted to the mobile device 100 over the wireless connector system 108. It is noted that the wireless connector system 108 may include a wireless network, wireless gateway, and/or wide area network.

[0035] The server 106 receives the attachment request 110 and uses the identifying information contained within the attachment request 110 to locate the proper attachment 102. The server 106 contains computer instructions, such as a secure message processing module 112, to look inside the secure message 104 to locate the attachment 102. In order to look inside the secure message 104, decryption operations may need to take place. Location of the attachment 102 within the secure message 104 can be accomplished in many ways, such as by locating a MIME field that contains or is associated with the desired attachment.

[0036] Once located, the server 106 sends over the wireless connector system 108 the requested attachment 114 to the mobile device 100. The mobile device 100 can then use the transmitted attachment 114 in any way permitted for the attachment, such as to view the attachment 114 or play an audio attachment.

[0037] Fig. 4 illustrates an operational scenario wherein a mobile device accesses an attachment. At step 200, a mobile device receives a secure message. If the secure message has one or more attachments, then the mobile device typically displays an icon to the user in order to indicate that an attachment is associated with the message and can be provided to the user. The

server may provide an indication to the mobile device that the secure message has an attachment, and the server's indication is used by the mobile device to indicate to the mobile device's user that the secure message has an attachment. Additionally, it should be understood that there may be situations where an attachment is to be provided to a mobile device other than a user indicating a desire to retrieve an attachment. As an illustration, a mobile device may automatically retrieve an attachment based upon the message being opened.

[0038] If the attachment is to be retrieved, then at step 202 the mobile device provides a request to have the attachment provided to it. At step 204, the server receives the attachment request. The attachment request may use many different approaches to indicate which attachment(s) the mobile device wishes to receive. For example, the device can specify which attachment it is interested in by using a message attachment indexing system that the device and server both understand. When the user wishes to view an attachment in an S/MIME message, the device sends the appropriate attachment identifier to the server. The server performs an index lookup to find the attachment or the message containing the attachment based upon the identifier.

[0039] At step 206, the server processes the secure message encoding and finds the attachment within the secure message. At step 208, the server provides the attachment to the mobile device. The mobile device provides the attachment to the user at step 210. It should be understood that the steps in the flowchart need not necessarily include all of the steps disclosed herein and may include further steps and operations. For example, the server may initially look inside the secure message, such as by decrypting the secure message, to determine whether any attachments are associated with the secure message. The server can provide an indication to the mobile device as to whether the secure message contained any attachments (which indication can then be provided to the user).

[0040] As another example, the server may render the attachment before transmitting it to the mobile device. As shown in Fig. 5, the server 106 may render the attachment 102 so that the attachment 102 can be more easily viewed (provided that the attachment is of the type that can be viewed by the mobile device). A rendering operation software module 300 accessible by the server 106 can perform the proper rendering of the attachment 102 so that the resource-limited mobile device 100 does not have to perform such operations.

[0041] The rendering operation software module 300 renders the attachment 102 so as to be compatible with the attachment viewing software used by the mobile device 100. If needed, module 300 can access a lookup table to determine which format to use to render the attachment 102 for a particular mobile device 100. It should be understood that other approaches may be used, such as the mobile device 100 indicating to the server 106 which format should be used to render the attachment 102, or the server 106 providing attachment viewing software to the mobile device 100 so that the mobile device 100 may view the rendered attachment 114.

[0042] The rendered attachment 114 is transmitted to the mobile device 100 and viewed normally on the mobile device 100. The server 106 may transmit all or a portion of the attachment 102. In the situation of the latter, if the mobile device 100 wants to see additional portions of the attachment 102, then the server 106 will send additional portions of the attachment 102 in response to a request by the mobile device 100.

[0043] Other operations can be performed with respect to the secure message and its attachment(s). For example, if a message is just signed, then the server can process the secure message encoding and find the attachment. However, if the message is encrypted, then the server uses one or more symmetric/asymmetric keys that are needed to decrypt the secure message.

[0044] As shown in Fig. 6, the mobile device 100 may provide the session key 402 (which was used to encrypt the secure message 104) to the server 106 with the attachment request 110. The server 106 accesses an encryption/decryption processing module 400 to decrypt the secure message 104 using the transmitted session key 402. After the secure message 104 had been decrypted by the module 400, the secure message processing module 112 looks into the secure message 104 and obtains the attachment 102. The attachment 302 is transmitted for use by the mobile device 100. The attachment 302 is optionally rendered as described above before transmission to the mobile device 100.

[0045] It will be appreciated that the systems and methods are disclosed by way of example only. Many variations on the systems and methods described above are within the scope of the invention as claimed, whether or not expressly described. For example, the operations disclosed herein may be implemented as the secure message processing module may comprise one or more modules in order to handle a secure message and its attachment(s). Data structures may be used as part of the operations, such as to store data needed to access the attachment contained within a secure message. Still further, data signals transmitted using a communication channel may be used with the systems and methods. The data signals can include any type of data, such as the data and attachments transmitted to and/or from a mobile device. The data signal may be packetized data that is transmitted through a carrier wave or other medium across the network. Computer-readable media may be provided to and used with the mobile device that is capable of causing a mobile device to perform the methods and implement the systems disclosed herein.

[0046] As another example, the methods and systems may be used with a wide assortment of electronic devices, such as a personal digital assistant (PDA) device or the mobile device 600 shown in FIG 7. With ref-

erence to Fig. 7, the mobile device 600 is preferably a two-way communication device having at least voice and data communication capabilities. The mobile device 600 preferably has the capability to communicate with other computer systems on the Internet. Depending on the functionality provided by the device, the device may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance or a data communication device (with or without telephony capabilities).

[0047] The mobile device 600 includes a transceiver 611, a microprocessor 638, a display 622, non-volatile memory 624, RAM 626, auxiliary input/output (I/O) devices 628, a serial port 630, a keyboard 632, a speaker 634, a microphone 636, a short-range wireless communications sub-system 640, and other device sub-systems 642. The transceiver 611 includes transmit and receive antennas 616, 618, a receiver (Rx) 612, a transmitter (Tx) 614, one or more local oscillators (LOs) 613, and a digital signal processor (DSP) 620. Within the non-volatile memory 624, the mobile device 600 includes a plurality of software modules 624A-624N that can be executed by the microprocessor 638 (and/or the DSP 620), including a voice communication module 624A, a data communication module 624B, and a plurality of other operational modules 624N for carrying out a plurality of other functions.

[0048] As described above, the mobile device 600 is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device 600 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in Fig. 7 by the communication tower 619. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network.

[0049] The communication subsystem 611 is used to communicate with the network 619. The DSP 620 is used to send and receive communication signals to and from the transmitter 614 and receiver 612, and may also exchange control information with the transmitter 614 and receiver 612. If the voice and data communications occur at a single frequency, or closely-spaced set of frequencies, then a single LO 613 may be used in conjunction with the transmitter 614 and receiver 612. Alternatively, if different frequencies are utilized for voice communications versus data communications, then a plurality of LOs 613 can be used to generate a plurality of frequencies corresponding to the network 619. Although two antennas 616, 618 are depicted in Fig. 7, the mobile device 600 could be used with a single antenna structure. Information, which includes both voice and data information, is communicated to and from the communication module 611 via a link between the DSP 620 and the microprocessor 638.

[0050] The detailed design of the communication subsystem 611, such as frequency band, component selection, power level, etc., will be dependent upon the communication network 619 in which the mobile device 600 is intended to operate. For example, a mobile device 600 intended to operate in a North American market may include a communication subsystem 611 designed to operate with the Mobitex or DataTAC mobile data communication networks and also designed to operated with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 600 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device 600.

[0051] Depending upon the type of network 619, the access requirements for the dual-mode mobile device 600 may also vary. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each device. In GPRS data networks, however, network access is associated with a subscriber or user of a mobile device 600. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate the mobile device 600 on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM, but the mobile device 600 will be unable to carry out any functions involving communications over the network 619, other than any legally required operations, such as '911' emergency calling.

[0052] After any required network registration or activation procedures have been completed, the mobile device 600 may send and receive communication signals, preferably including both voice and data signals, over the network 619. Signals received by the antenna 616 from the communication network 619 are routed to the receiver 612, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding to be performed using the DSP 620. In a similar manner, signals to be transmitted to the network 619 are processed, including modulation and encoding, for example, by the DSP 620 and are then provided to the transmitter 614 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 619 via the antenna 618. Although a single transceiver 611 is shown in Fig. 7 for both voice and data communications, the mobile device 600 may include two distinct transceivers, a first transceiver for transmitting and receiving voice signals, and a second transceiver for transmitting and receiving data signals.

[0053] In addition to processing the communication

signals, the DSP 620 also provides for receiver and transmitter control. For example, the gain levels applied to communication signals in the receiver 612 and transmitter 614 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 620. Other transceiver control algorithms could also be implemented in the DSP 620 in order to provide more sophisticated control of the transceiver 611.

[0054] The microprocessor 638 preferably manages and controls the overall operation of the mobile device 600. Many types of microprocessors or microcontrollers could be used for this part, or, alternatively, a single DSP 620 could be used to carry out the functions of the microprocessor 638. Low-level communication functions, including at least data and voice communications, are performed through the DSP 620 in the transceiver 611. Other, high-level communication applications, such as a voice communication application 624A, and a data communication application 624B may be stored in the non-volatile memory 624 for execution by the microprocessor 638. For example, the voice communication module 624A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 600 and a plurality of other voice devices via the network 619. Similarly, the data communication module 624B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 600 and a plurality of other data devices via the network 619.

[0055] The microprocessor 638 also interacts with other device subsystems, such as the display 622, non-volatile memory 624, random access memory (RAM) 626, auxiliary input/output (I/O) subsystems 628, serial port 630, keyboard 632, speaker 634, microphone 636, a short-range communications subsystem 640 and any other device subsystems generally designated as 642. The components 628, 632, 634 and 636 are examples of the types of subsystems that could be provided as users interfaces. The modules 624A-N are executed by the microprocessor 638 and may provide a high-level interface between a user of the mobile device and the mobile device. This interface typically includes a graphical component provided through the display 622, and an input/output component provided through the auxiliary I/O 628, keyboard 632, speaker 634, or microphone 636.

[0056] Some of the subsystems shown in Fig. 7 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 632 and display 622 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

[0057] Operating system software used by the microprocessor 638 is preferably stored in a persistent store such as non-volatile memory 624. In addition to the operating system and communication modules 624A-N, the non-volatile memory 624 may also include a file system for storing data. A storage area is also preferably provided in the non-volatile memory 624 to store public keys, a private key, and other information required for secure messaging. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 626 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 626 before permanently writing them to a file system located in the non-volatile store 624. As those skilled in the art will appreciate, the non-volatile store 624 may be implemented as a Flash memory component or a battery backed-up RAM, for example.

[0058] An exemplary application module 624N that may be loaded onto the mobile device 600 is a personal information manager (PIM) application providing PDA functionality, such as calendar events, appointments, and task items. This module 624N may also interact with the voice communication module 624A for managing phone calls, voice mails, etc., and may also interact with the data communication module 624B for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 624A and the data communication module 624B may be integrated into the PIM module.

[0059] The non-volatile memory 624 preferably provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 624A, 624B, via the wireless network 619. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless network 619, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

[0060] The mobile device 600 may also be manually synchronized with a host system by placing the mobile device 600 in an interface cradle, which couples the serial port 630 of the mobile device 600 to the serial port of the host system. The serial port 630 may also be used to download other application modules 624N for installation, and to load Certs, keys and other information onto a device. This wired download path may be used to load an encryption key onto the mobile device 600, which is a more secure method than exchanging encryption information via the wireless network 619.

[0061] Additional application modules 624N may be loaded onto the mobile device 600 through the network 619, through an auxiliary I/O subsystem 628, through the serial port 630, through the short-range communications subsystem 640, or through any other suitable subsystem 642, and installed by a user in the non-volatile memory 624 or RAM 626. Such flexibility in appli-

cation installation increases the functionality of the mobile device 600 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 600.

[0062] When the mobile device 600 is operating in a data communication mode, a received signal, such as a text message or a web page download, is processed by the transceiver 611 and provided to the microprocessor 638, which preferably further processes the received signal for output to the display 622, or, alternatively, to an auxiliary I/O device 628. A user of mobile device 600 may also compose data items, such as email messages, using the keyboard 632, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 600 is further enhanced with a plurality of auxiliary I/O devices 628, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user may then be transmitted over the communication network 619 via the transceiver 611.

[0063] When the mobile device 600 is operating in a voice communication mode, the overall operation of the mobile device 600 is substantially similar to the data mode, except that received signals are preferably output to the speaker 634 and voice signals for transmission are generated by a microphone 636. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the mobile device 600. Although voice or audio signal output is preferably accomplished primarily through the speaker 634, the display 622 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 638, in conjunction with the voice communication module 624A and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 622.

[0064] A short-range communications subsystem 640 is also included in the mobile device 600. For example, the subsystem 640 may include an infrared device and associated circuits and components, or a short-range wireless communication module such as a Bluetooth™ communication module or an 802.11 module to provide for communication with similarly-enabled systems and devices. Those skilled in the art will appreciate that "Bluetooth" and "802.11" refer to sets of specifications, available from the Institute of Electrical and Electronics Engineers (IEEE), relating to wireless personal area networks and wireless LANs, respectively.

Claims

1. A method for handling secure message attachments for a mobile device, comprising the steps of:

   receiving at a server a second attachment provided within a secure message;

   wherein the secure message itself was received by the server as a first attachment;

   requesting the second attachment at the mobile device;

   processing the secure message in order to locate within the secure message the second attachment; and

   providing the second attachment to the mobile device.

2. The method of claim 1, wherein the secure message is structured according to a security scheme such that the secure message is handled as an attachment by the server.

3. The method of claim 2, wherein the security scheme includes a symmetric key scheme.

4. The method of claim 2, wherein the security scheme includes an asymmetric key scheme.

5. The method of claim 2, wherein the security scheme is a Secure Multipurpose Internet Mail Extensions (S/MIME) scheme.

6. The method according to one of the claims 1 to 5, wherein the secure message is structured such that a secure layer has been added to the message and the second attachment.

7. The method of claim 6, wherein the secure layer acts as an envelope with respect to the message and the second attachment.

8. The method according to one of the claims 6 to 7, wherein the secure layer was generated during an encryption operation.

9. The method according to one of the claims 6 to 8, wherein a session key is received by the server from the mobile device for use by the server to decrypt the secure message.

10. The method according to one of the claims 6 to 9 , wherein the secure layer was generated during a digital signature operation.

11. The method according to one of the claims 6 to 10, wherein the secure layer was generated during an encryption operation.

12. The method according to one of the claims 1 to 11, wherein the second attachment is selected from the group consisting of: a textual document, word processing document, audio file, image file, or video file.

13. The method according to one of the claims 1 to 12, wherein the secure message without the second attachment is sent from the server to the mobile device, wherein the second attachment is provided to the mobile device based upon the mobile device requesting the second attachment.

14. The method of claim 13, wherein the request from the mobile device for the second attachment results from a user requesting the second attachment.

15. The method of claim 13, wherein the request from the mobile device includes data to be used by the server to identify the second attachment that is to be provided to the mobile device.

16. The method according to one of the claims 1 to 15, wherein the secure layer was generated during an encryption operation, wherein a decryption operation is performed in order to locate within the secure message the second attachment.

17. The method according to one of the claims 1 to 16, wherein the secure message has a plurality of attachments.

18. The method according to one of the claims 1 to 17, wherein the server provides an indication to the mobile device that the secure message has the second attachment,
wherein the indication is used by the mobile device to indicate to the mobile device's user that the secure message has the second attachment.

19. The method according to one of the claims 1 to 18, wherein the second attachment is automatically provided by the server to the mobile device when the secure message is opened by the mobile device's user.

20. The method according to one of the claims 1 to 19, wherein the second attachment is rendered before being provided to the mobile device.

21. The method according to one of the claims 1 to 20, wherein means for providing a wireless network and means for providing a message server are used to communicate the located attachment to the mobile device.

22. The method according to one of the claims 1 to 21, wherein the mobile device is a handheld wireless mobile communications device.

23. The method according to one of the claims 1 to 22, wherein the mobile device is a personal digital assistant (PDA).

24. An apparatus located at a computer server for handling secure message attachments for a mobile device, wherein the server receives a secure message containing a second attachment, comprising:

a data store that stores the secure message and the second attachment;

wherein the secure message contains a secure layer such that the secure message itself is received by the server as a first attachment;

a secure message processing module that looks into the secure message through the secure layer in order to locate the second attachment;

wherein the second attachment is provided to the mobile device.

25. The apparatus of claim 24, further comprising:

a rendering module that renders the second attachment before the second attachment is provided to the mobile device.

26. The apparatus according of one of the claims 24 to 25, further comprising:

a decryption processing module to decrypt the secure message so that the second attachment can be located within the secure message.

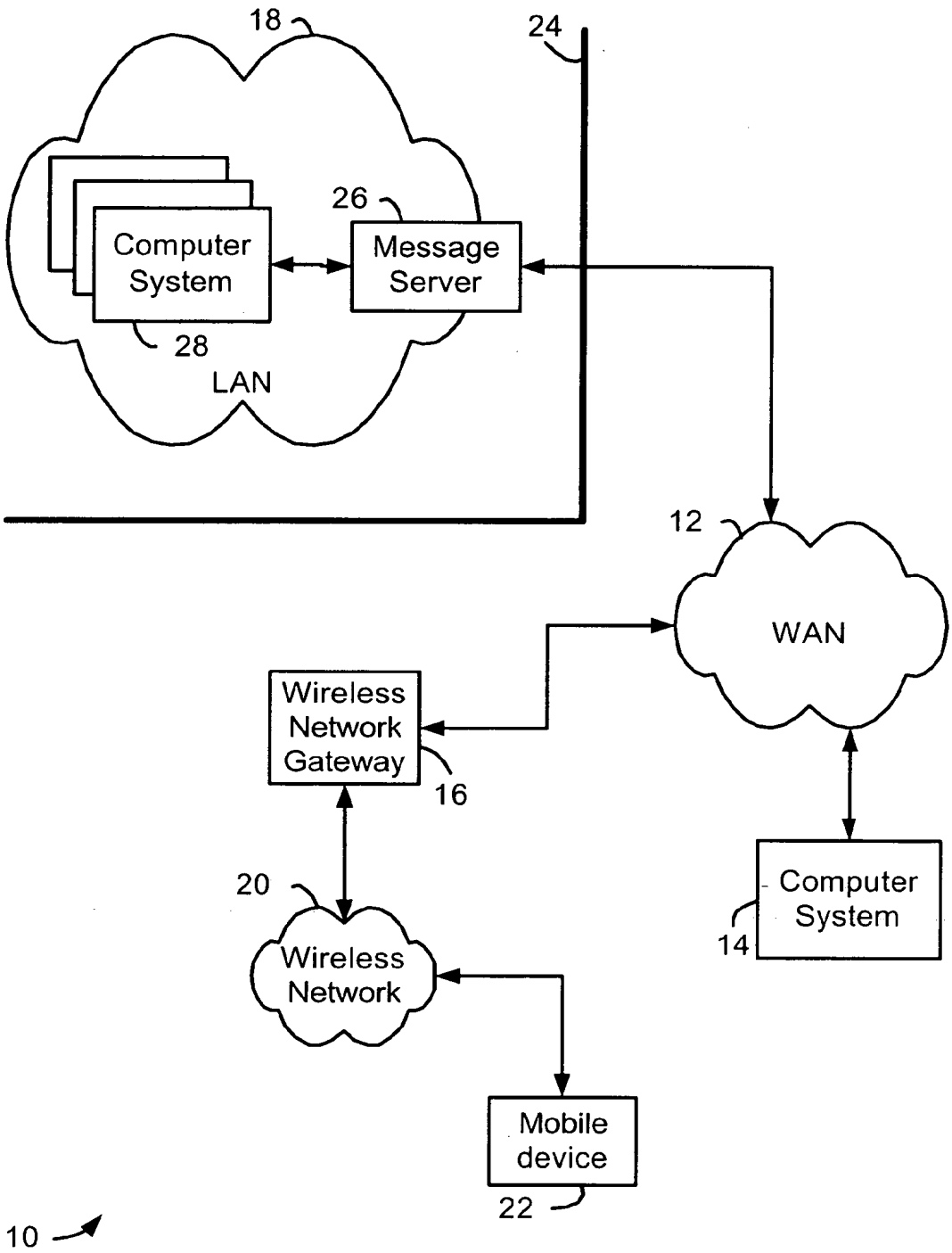
18
24
26
Computer System
Message Server
28
LAN
12
WAN
Wireless Network Gateway
16
20
Wireless Network
Computer System
14
Mobile device
22
10

FIG. 1

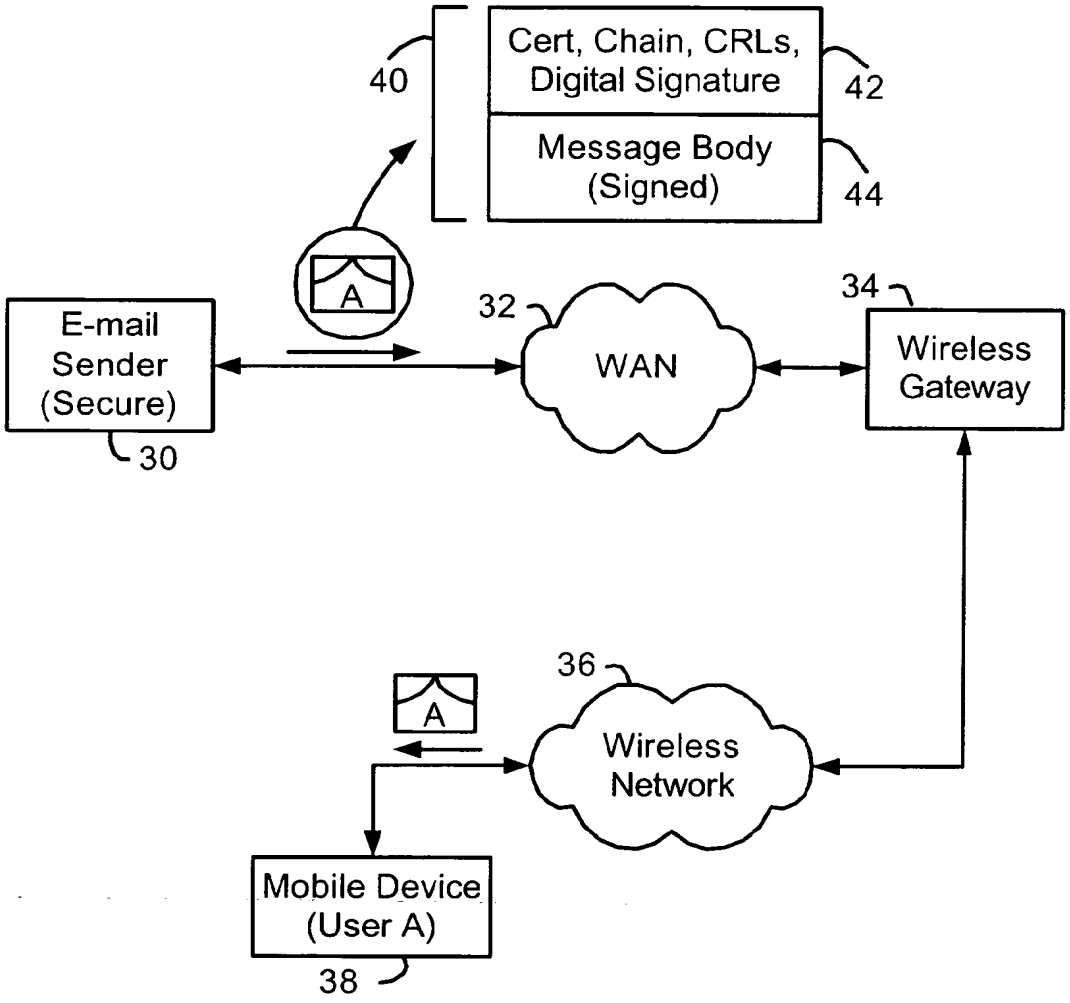
Cert, Chain, CRLs, Digital Signature
42
40
Message Body (Signed)
44
A
E-mail Sender (Secure)
30
32
WAN
34
Wireless Gateway
36
A
Wireless Network
Mobile Device (User A)
38

FIG. 2

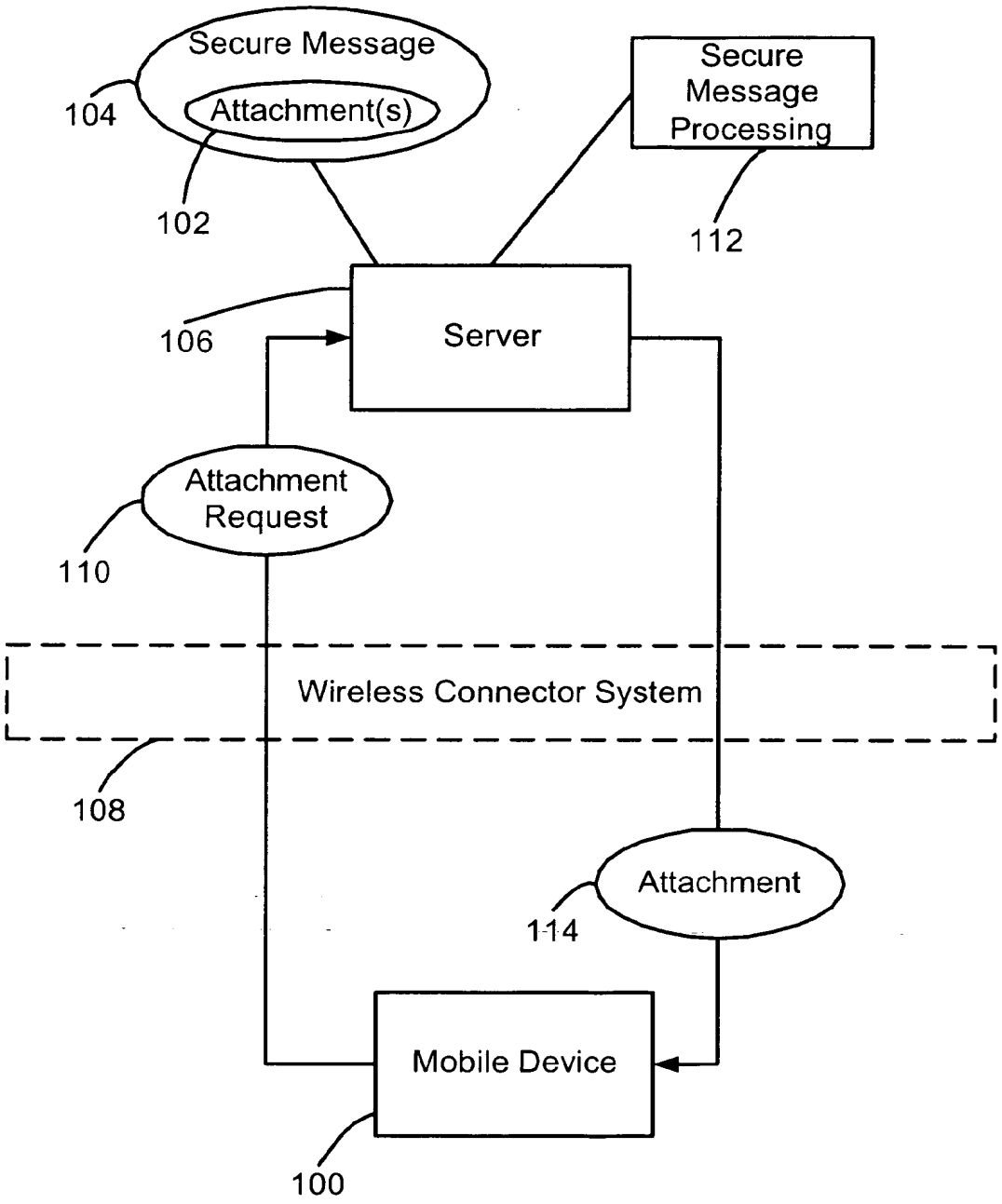
Secure Message
Attachment(s)
104
102
Secure Message Processing
112
Server
106
Attachment Request
110
Wireless Connector System
108
Attachment
114
Mobile Device
100

FIG. 3

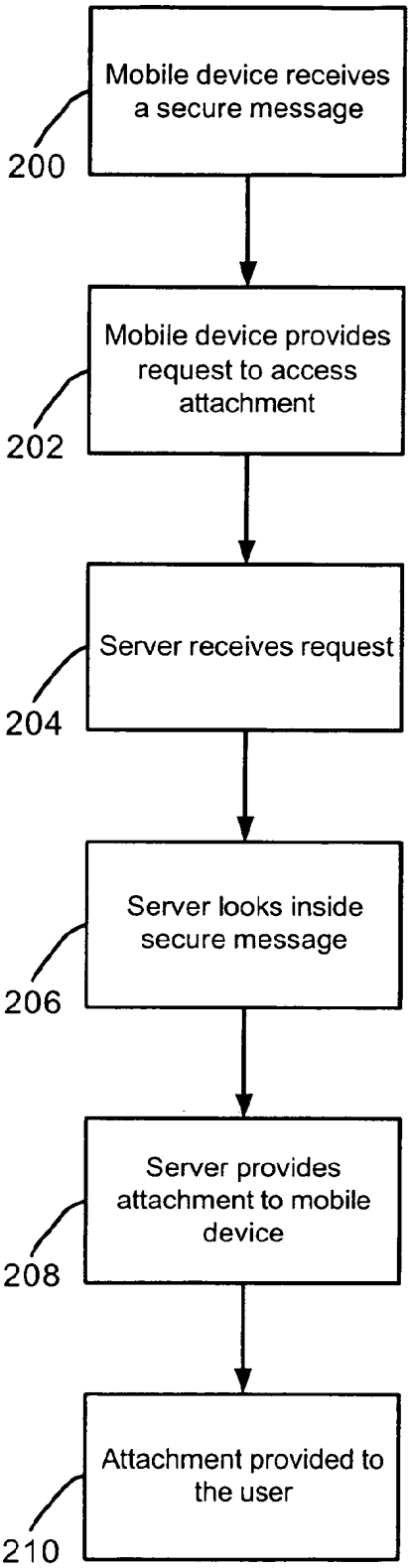
Mobile device receives a secure message
200
Mobile device provides request to access attachment
202
Server receives request
204
Server looks inside secure message
206
Server provides attachment to mobile device
208
Attachment provided to the user
210

FIG. 4

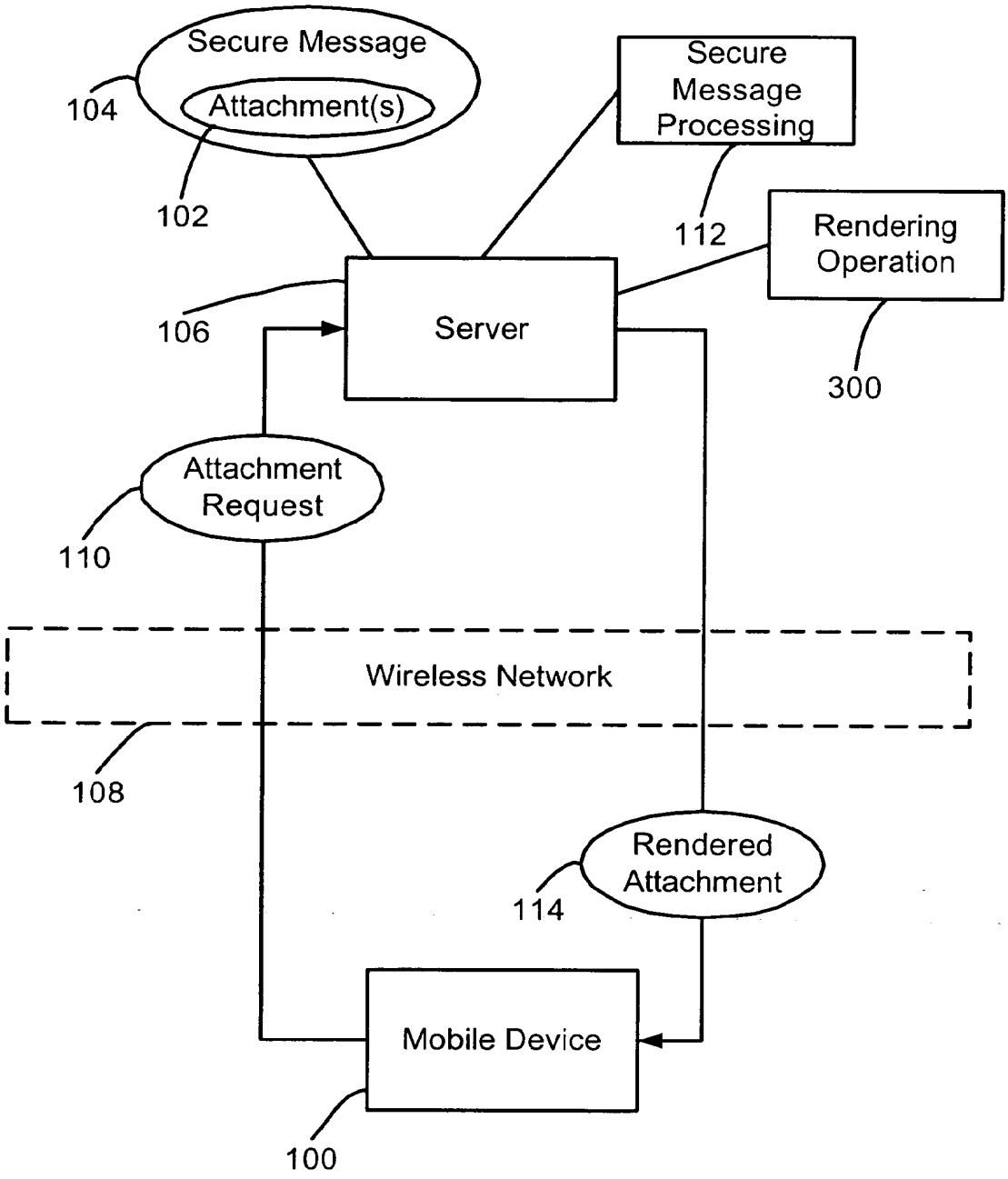
Secure Message
Attachment(s)
104
102
Secure Message Processing
112
Rendering Operation
300
106
Server
Attachment Request
110
Wireless Network
108
Rendered Attachment
114
Mobile Device
100

FIG. 5

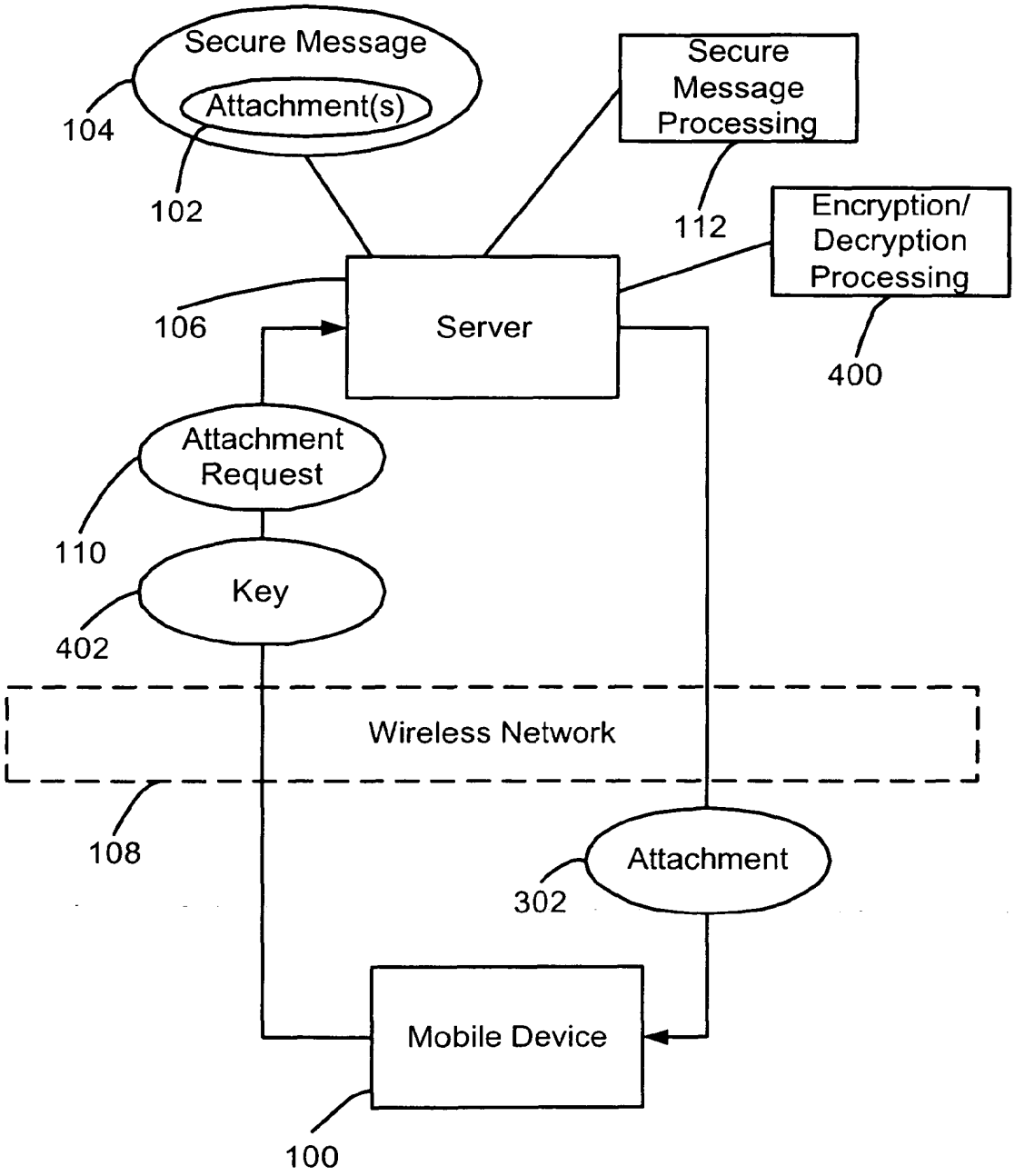
Secure Message
Attachment(s)
104
102
Secure Message Processing
112
Encryption/ Decryption Processing
400
106
Server
Attachment Request
110
Key
402
Wireless Network
108
Attachment
302
Mobile Device
100

FIG. 6

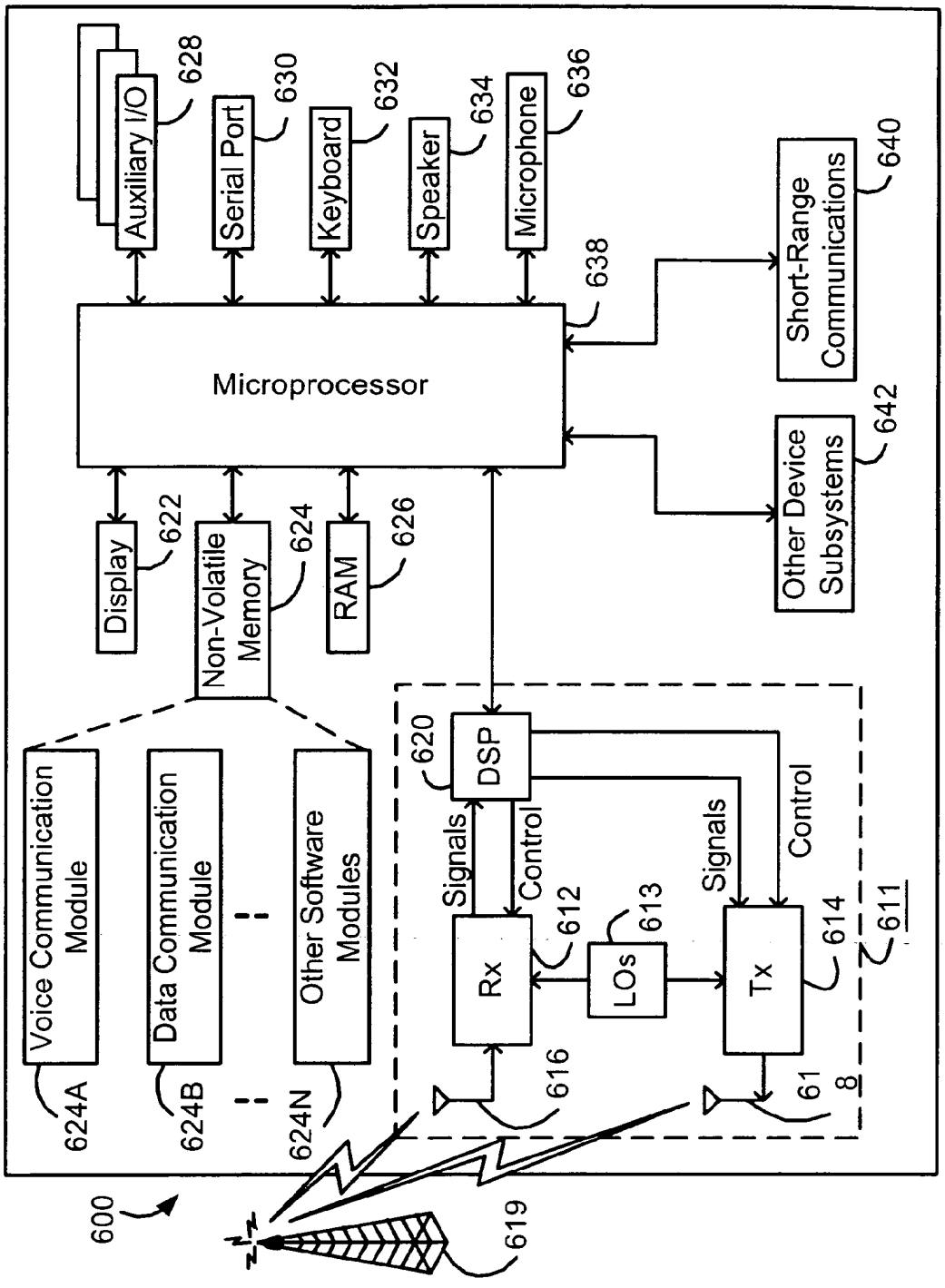
600
Auxiliary I/O
628
Serial Port
630
Keyboard
632
Speaker
634
Microphone
636
638
Microprocessor
Short-Range Communications
640
Other Device Subsystems
642
Display
622
Non-Volatile Memory
624
RAM
626
Voice Communication Module
Data Communication Module
Other Software Modules
624A
624B
624N
DSP
620
Signals
Control
Rx
612
LOs
613
Signals
Control
Tx
614
611
616
618
619

FIG. 7

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 00 6851

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 02/101580 A (RES IN MOTION LTD ; ADAMS NEIL P (CA); BROWN MICHAEL S (CA); GODFREY J) 19 December 2002 (2002-12-19) * page 1, line 12 - page 2, line 12 * * page 6, line 12 - line 18 * * page 7, line 2 - line 22 * * page 8, line 21 - page 12, line 21 * * page 14, line 10 - line 16 * * page 35, line 5 - line 21 * * figure 2 * -----	1-26	H04L29/06 H04L12/58
A	WO 2004/010661 A (WITNESS INC E ; ROBERTS MICHAEL (CA); WAUGH DONALD (CA); VIATCHESLAV I) 29 January 2004 (2004-01-29) * abstract * * page 2, line 7 - line 28 * * page 4, line 21 - page 5, line 9 * * page 7, line 1 - line 5 * * page 8, line 15 - page 13, line 2 * * page 14, line 15 - page 16, line 24 * -----	1-26	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
A	WO 03/058483 A (GUSTAFSON BRIAN D ; BOYNTON LEE R (US); BURKE SCOTT M (US); DUNCAN FRE) 17 July 2003 (2003-07-17) * page 1, line 7 - line 18 * * page 6, line 14 - line 23 * * page 8, line 5 - page 9, line 17 * * page 12, line 7 - line 12 * -----	1-26	H04L
A	STALLINGS W: "S/MIME: E-MAIL GETS SECURE" BYTE, MCGRAW-HILL INC. ST PETERBOROUGH, US, vol. 23, no. 7, 1 July 1998 (1998-07-01), pages 41-42, XP000774260 ISSN: 0360-5280 * the whole document * -----	1-26	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	5 August 2004	Kopp, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 00 6851

This annex lists the patent family members relating to the patent documents cited in the above-mentioned Europcan search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-08-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02101580 A	19-12-2002	WO 02101580 A1	19-12-2002
		WO 02101605 A2	19-12-2002
		WO 02102009 A2	19-12-2002
		CA 2450584 A1	19-12-2002
		CA 2450601 A1	19-12-2002
		CA 2450631 A1	19-12-2002
		EP 1410293 A2	21-04-2004
		EP 1399853 A1	24-03-2004
		EP 1410296 A2	21-04-2004
WO 2004010661 A	29-01-2004	CA 2394451 A1	23-01-2004
		WO 2004010661 A1	29-01-2004
		US 2004019780 A1	29-01-2004
WO 03058483 A	17-07-2003	WO 03058483 A1	17-07-2003
		WO 03058879 A1	17-07-2003
		US 2003157947 A1	21-08-2003
		US 2003235308 A1	25-12-2003

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82